In the previous article in this short series, Robert Gezelter, CDP, has been discussing the importance of the Domain Name System (DNS) in ensuring continued service for one’s Internet domain and Web site.

* * *

The most rudimentary step for continued functioning of one’s Internet site or Web site is that there should always be at least a distinct primary and secondary DNS server of the domain. For a production domain, this means that the minimum two name servers should be distinct systems located in different locations. This answers the common question “Can I use multi-hosting to get the two name servers I require for my domain?” The answer is a resounding “NO.” The reason for the two-server rule (which is implemented with varying degrees of thoroughness by different domain registrars) is to ensure that there are at least two discrete sources for DNS data.

This author has seen organizations that were able to circumvent their domain registrar’s safety checks by using two DNS names that resolved to the same address. However, when a cable fault disconnected such a DNS-hosting organization from the Internet, the data from their single DNS server became unavailable. This resulted in a multi-hour outage at the WWW servers located at a service provider whose name was supposed to be resolved by the unreachable DNS server. Switching to a different DNS server would have required a change to the data dispensed by the root name servers, which are updated on, at best, a daily basis (the propagation delay between an update made at a zone’s registrar and the root servers depends upon the day of the week and the registrar). Therefore the disappearance of the DNS service was not correctable in a timely manner and the Web site was down until cable fault was repaired.

Production DNS servers should be geographically dispersed. A pair of workstations located next to each other, plugged into the same power-strip is a fool’s dispersion; all but the most trivial incidents will result in both servers becoming unavailable. Achieving geographic diversity is neither difficult nor expensive. It does not require resorting to a DNS server provided by a separate hosting service or by an ISP (although a hosting- or ISP-provided DNS server is certainly a possible alternative). A field office or sister organization can easily provide the few cubic feet and kilobytes per hour (yes, per hour) required to domicile an alternate DNS server. The system can be managed remotely. Reciprocal arrangements between organizations (I will host a secondary on my name server if you host my secondary on yours) are even simpler. Providing a separate DSL circuit for the use of the alternate DNS server is much cheaper to an enterprise than losing its name-resolution services (i.e., effectively having one’s entire domain disconnected from the Internet).

If a site is a serious production site, many concurrent users, more extensive monitoring is both justified and prudent. Each link of the chain connecting customers to the site should be monitored on some basis sufficient to alert the organization to a problem in a timely manner. In the case of DNS servers, regular verification that the name servers are online and responding
properly is a prudent precaution.

Diversity of carriers, geographic location, and routing are important steps to ensuring that single-source errors (personnel accidents, natural or man-made disasters, or organizational errors) do effectively terminate your domain’s DNS services and impair the overall Internet accessibility of domain members.

In summary, the analogy to a fabric or web is both simple and straightforward: an individual thread or moderate number of threads in a fabric may break, without compromising the ability of the fabric as a whole to perform its function. In addition, breaks in the fabric that can be detected without becoming apparent to customers can inherently be corrected without customer impact. Dispersion of functionality is far cheaper, and is far more resilient than attempts to harden facilities beyond the possibility of damage.

* * *

Robert Gezelter, CDP (mailto:gezelter@rlgsc.com) is the founding principal of the consulting firm which bears his name (http://www.rlgsc.com). His over 25 years of experience includes consulting to clients locally, nationally, and internationally. He is a frequent speaker on technical topics at conferences in the US and internationally. He has previously published articles in Network World, Open Systems Today, Digital Systems Journal, Digital News, and Hardcopy. He is also a contributor to the _Computer Security Handbook, 4th Edition_ (3 chapters, Wiley, 2002), and its 1995 predecessor.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www3.norwich.edu/msia > for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2003 Robert L. Gezelter. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.